

UNITED STATES DISTRICT COURT
DISTRICT OF SOUTH DAKOTA
SOUTHERN DIVISION

In the Matter of the Search Regarding No. 4:21-mj-22

21-020-04

SEARCH AND SEIZURE WARRANT
"REDACTED"

TO: ANY AUTHORIZED LAW ENFORCEMENT OFFICER

An application by a federal law enforcement officer or an attorney for the government requests the search of records fully described in Attachment A, attached hereto and incorporated herein by reference.

I find that the affidavit, or any recorded testimony, establish probable cause to search and seize the property described above, and that such search will reveal evidence of the commission of criminal offenses, contraband, the fruits of crime, or things otherwise criminally possessed, or property designed or intended for use or which is or has been used as the means of committing criminal offenses concerning violations of 21 U.S.C. §§ 841(a)(1) and 846 and 18 U.S.C. § 1956, as fully described in Attachment B, attached hereto and incorporated herein by reference.

YOU ARE COMMANDED to execute this warrant on or before

March 3, 2021 (not to exceed 14 days)

☒ in the daytime - 6:00 a.m. to 10:00 p.m.

☐ at any time in the day or night as I find reasonable cause has been established.

Unless delayed notice is authorized below, you must give a copy of the warrant and a receipt for the property taken to the person from whom, or from whose premises, the property was taken, or leave the copy and receipt at the place where the property was taken.

The officer executing this warrant, or an officer present during the execution of the warrant, must prepare an inventory as required by law and promptly return this warrant and inventory to the undersigned Judge.

☐ Pursuant to 18 U.S.C. § 3103a(b), I find that immediate notification may have an adverse result listed in 18 U.S.C. § 2705 (except for delay of trial), and authorize the officer executing this warrant to delay notice to the person who, or whose property, will be searched or seized,

- ☐ for _____ days (*not to exceed 30*).
- ☐ until, the facts justifying, the later specific date of _____.

Issued telephonically 2-17-21 at 8:45^{am} CST at Sioux Falls, South Dakota
Date and Time Issued



VERONICA L. DUFFY
UNITED STATES MAGISTRATE JUDGE

UNITED STATES DISTRICT COURT
DISTRICT OF SOUTH DAKOTA
SOUTHERN DIVISION

In the Matter of the Search Regarding

No. 4:21-mj-22

21-020-04

RETURN "REDACTED"

Date and time warrant executed: _____

Copy of warrant and inventory left with: _____

Inventory made in the presence of: _____

Inventory of the property taken and name of any person(s) seized (attach additional sheets, if necessary):

<p style="text-align: center;">CERTIFICATION</p> <p>I declare under penalty of perjury that this inventory is correct and was returned along with the original warrant to the designated judge.</p> <p style="text-align: right;">_____ Craig Scherer, Special Agent Homeland Security Investigations</p>
--

UNITED STATES DISTRICT COURT
DISTRICT OF SOUTH DAKOTA
SOUTHERN DIVISION

In the Matter of the Search Regarding No. 4:21-mj-22

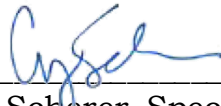
21-020-04

**APPLICATION FOR SEARCH AND
SEIZURE WARRANT "REDACTED"**

I, Craig Scherer, being duly sworn depose and say:

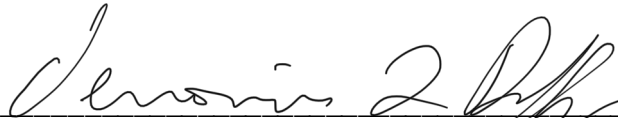
I am a Special Agent with the United States Department of Homeland Security (DHS), Immigration and Customs Enforcement (ICE), Homeland Security Investigations (HSI), and have reason to believe that within the records fully described in Attachment A, attached hereto and incorporated herein by reference, there is now concealed certain property, namely: that fully described in Attachment B, attached hereto and incorporated herein by reference, which I believe is property constituting evidence of the commission of criminal offenses, contraband, the fruits of crime, or things otherwise criminally possessed, or property designed or intended for use or which is or has been used as the means of committing criminal offenses concerning violations of 21 U.S.C. §§ 841(a)(1) and 846 and 18 U.S.C. § 1956.

The facts to support a finding of Probable Cause are contained in my Affidavit filed herewith.



Craig Scherer, Special Agent
Homeland Security Investigations

Subscribed and sworn to telephonically on the 17th day of February, 2021.



VERONICA L. DUFFY
UNITED STATES MAGISTRATE JUDGE

UNITED STATES DISTRICT COURT
DISTRICT OF SOUTH DAKOTA
SOUTHERN DIVISION

In the Matter of the Search Regarding No. 4:21-mj-22

21-020-04

**AFFIDAVIT IN SUPPORT OF
SEARCH AND SEIZURE WARRANT
"REDACTED"**

STATE OF SOUTH DAKOTA)
 :SS
COUNTY OF MINNEHAHA)

I, Craig Scherer, being duly sworn on oath, depose and say:

INTRODUCTION AND AGENT BACKGROUND

1. I am a Special Agent with the United States Department of Homeland Security (DHS), Immigration and Customs Enforcement (ICE), Homeland Security Investigations (HSI) in Sioux Falls, South Dakota and have been duly employed in this position since December 2003. I am a graduate of the Criminal Investigator Training Program and ICE Special Agent Training Program at the Federal Law Enforcement Training Center. I have received specialized training pertaining to conducting criminal investigations, immigration and customs laws, investigative techniques, searching databases, conducting interviews, executing search warrants, and making arrests with respect to criminal violations of United States Code.

2. As a Special Agent one of my responsibilities is investigating drug trafficking organizations and associated money laundering methods. I have assisted with numerous investigations into violations of the Federal Controlled Substances Act and I am familiar with the provisions of Title 21 and 18 of the United States Code. I have been working drug trafficking cases since 2005.

PURPOSE OF AFFIDAVIT

3. Through this affidavit, I am requesting a search warrant be issued for all contents of the Apple account associated with [REDACTED] ("SUBJECT ACCOUNT"), that are stored at premises owned, maintained, controlled, or operated by Apple, Inc., a business with offices located at 1 Infinite Loop, Cupertino, CA 95014-2084.

4. As described more fully below, I respectfully submit there is probable cause to believe that the information associated with the SUBJECT ACCOUNT constitutes evidence or instrumentalities of criminal violations of

21 U.S.C. §§ 841 and 846 – Conspiracy to Possess With Intent to Distribute a Controlled Substance and 18 U.S.C. § 1956 – Money Laundering.

5. Because this affidavit is being submitted for the limited purpose of securing a search warrant, I have not included each and every fact known to me concerning this investigation. I have set forth only those facts that I believe are necessary to establish probable cause to believe that evidence of violations of United States Code are located within the accounts described in this affidavit.

6. I have received information from other law enforcement officers and sources of information by either verbal or written report. The officers and sources providing information may have received the information by way of personal knowledge or from another source.

SUMMARY OF INVESTIGATION

7. HSI Sioux Falls, IRS and the Sioux Falls Area Drug Task Force (SFADTF) have been investigating an international methamphetamine Drug Trafficking Organization (DTO) responsible for sending bulk methamphetamine from California to South Dakota. This organization is also suspected of laundering proceeds through various methods.

8. Through interviews, controlled purchase of methamphetamine, search warrants, surveillance, phone toll analysis and other law enforcement activities, Canbie THOMPSON was identified as a high-level participant of the DTO.

9. THOMPSON was the focus of a prior HSI Sioux Falls methamphetamine investigation involving methamphetamine distribution by Asian street gang members. In 2011, THOMPSON was convicted in the District of South Dakota for violations of 21 U.S.C. §§ 841 and 846 and sentenced to 126 months imprisonment.

10. In April 2020, SFADTF Detective Dan Christiansen conducted an interview of Source of Information (SOI) [REDACTED]. The SOI's identity is known to Detective Christiansen, however they requested to remain anonymous. The SOI stated [REDACTED]

[REDACTED]

11. Sioux Falls Police Department (SFPD) record checks identified THOMPSON's current phone number as [REDACTED] and current address as [REDACTED], Sioux Falls, SD. Detective Christiansen also verified THOMPSON resides at [REDACTED], through the property manager.

12. On October 26, 2020, Detective Christiansen spoke to another Source of Information (SOI-2) who wished to remain unnamed, however their identity is known to law enforcement. SOI-2 stated [REDACTED]
[REDACTED]

13. On November 3, 2020, and November 9, 2020, Detective Christiansen spoke with SFADTF Confidential Informant (CI) 20-19, who stated [REDACTED]
[REDACTED]

14. On November 20, 2020, HSI Sioux Falls received records responsive to a South Dakota Fusion Center query for THOMPSON. The query listed the following information:

South Dakota driver's license

- Driver's license: [REDACTED]
- SSN: [REDACTED]
- Address: [REDACTED] Lower Brule, SD
- Phone: [REDACTED]
- Email: [REDACTED] (SUBJECT ACCOUNT).

Registered vehicles in South Dakota

- 2016 white Chrysler 300 with South Dakota plate [REDACTED] and expiration of November 2021.
- 2003 blue Toyota Camry with South Dakota plate [REDACTED] and expiration of November 2021.

South Dakota wages

- THOMPSON's last reported wages were from the 3rd quarter of 2019 at Lev Group LLC and Fresh Farms LLC.

15. On November 30, 2020, FBI Task Force Officer Dylan Dowling conducted a proffer interview of [REDACTED] in [REDACTED]. The following information are excerpts of [REDACTED] interview as they relate to this investigation.

16. [REDACTED] stated [REDACTED]
[REDACTED]

[REDACTED]

17. [REDACTED] identified [REDACTED]

[REDACTED]

18. TFO Dowling also stated [REDACTED] is believed to be sourced by THOMPSON. HSI Sioux Falls Criminal Analyst (CA) Josh Hauck queried law enforcement databases and learned [REDACTED]

19. On November 30, 2020, CA Hauck conducted further record checks in law enforcement databases for financial transactions associated to THOMPSON. CA Hauck ran phone number [REDACTED] belonging to THOMPSON. A total of 24 records were returned between December 2017 and November 2020. Of the available records, THOMPSON [REDACTED]

[REDACTED]

20. A review of the outgoing transactions revealed between December 9, 2017 and November 13, 2020, THOMPSON [REDACTED]

[REDACTED] being convicted of conspiracy to distribute a controlled substance-methamphetamine and sentenced to 10 years.

21. On December 7, 2020, Detective Christiansen applied for and received a [REDACTED]

[REDACTED]

22. On December 10, 2020, CA Hauck conducted open source record checks for Enterprise rental car receipts associated to THOMPSON. The query

revealed between April 19, 2020 and November 2, 2020, [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

A high-contrast, black and white graphic design. On the left side, there is a vertical column of small, rectangular blocks, some of which are white and others black, creating a rhythmic pattern. The rest of the image is a solid black field.

24. On December 18, 2020, I received data from an active [REDACTED] for [REDACTED] based phone number [REDACTED] issued in the Eastern District of

Virginia. This phone number was identified as being in contact with THOMPSON. Exploitation of the data and subsequent searches in DHS indices resulted in the identification of [REDACTED] based and domestic phone numbers in contact with [REDACTED].

25. Between December 17, 2020 and December 21, 2020, [REDACTED] based phone number [REDACTED]. A search in law enforcement and DHS indices revealed Odalis [REDACTED] [REDACTED] was part of a prior HSI Yuma investigation. On March 1, 2017, [REDACTED] was arrested with \$17,860 U.S. currency and several firearms at the DeConcini Port of Entry in Nogales, AZ.

26. Between December 16, 2020 and December 19, 2020, [REDACTED] [REDACTED] A search in law enforcement and DHS indices revealed [REDACTED] [REDACTED]. On November 7, 2020, [REDACTED] [REDACTED]. The transaction originated in Sioux Falls, SD and was received in [REDACTED] Per SFADTF reporting, [REDACTED] is associated to the distribution of controlled substances.

27. On December 31, 2020, Detective Christiansen and South Dakota Division of Criminal Investigation SA Matt Glenn encountered [REDACTED]

28. [REDACTED] stated

29. [REDACTED] stated

[REDACTED]

30. [REDACTED] stated [REDACTED]

[REDACTED]

31. A review of THOMPSON available [REDACTED] revealed THOMPSON

[REDACTED]

[REDACTED]

32. HSI Sioux Falls served a subpoena on Verizon Wireless for subscriber details associated to THOMPSON's phone of [REDACTED]. The records revealed THOMPSON utilizes an Apple iPhone XS Max Gold 512GB phone with IMEI number [REDACTED].

33. On January 11, 2021, I applied for and received a federal search warrant from the District of South Dakota for THOMPSON's Apple iCloud account associated to [REDACTED]. On February 4, 2021, I received records from Apple in response to the search warrant.

34. A review of the Apple records identified [REDACTED]

[REDACTED] The records also included [REDACTED]. I believe THOMPSON continues to distribute methamphetamine and that THOMPSON's iCloud account contains additional evidence of drug trafficking.

35. Based on my training and experience, I know persons involved with drug trafficking often communicate with sources of supply and customers via multiple methods, including Apple iMessage, in order to elude detection by law enforcement.

36. Based on my training and experience, I know persons involved with drug trafficking often create and use pseudonyms in order to elude detection by law enforcement.

37. Based on my training and experience, I know that it is common for people involved in the sale, distribution and use of illegal drugs to keep records of their travel, customers and suppliers, sometimes in Apple accounts.

38. I know, based on my training and experience, that even if long-time drug traffickers stop distributing controlled substances, either voluntarily or under law enforcement pressure, these traffickers often retain in their possession many items with evidentiary value, including names, addresses and telephone numbers of associates; documents related to financial transactions; and other items as listed in this affidavit.

39. I believe the Apple account identified in this affidavit contains evidence of THOMPSON's drug trafficking and money laundering activities.

TECHNICAL BACKGROUND

40. Apple provides a variety of services that can be accessed from Apple devices or, in some cases, other devices via web browsers or mobile and desktop applications ("apps"). The services include email, instant messaging, and file storage.

41. iMessage and FaceTime allow users of Apple devices to communicate in real-time. iMessage enables users of Apple devices to exchange instant messages ("iMessages") containing text, photos, videos, locations, and contacts, while FaceTime enables those users to conduct video calls.

42. iCloud is a file hosting, storage, and sharing service provided by Apple. iCloud can be utilized through numerous iCloud-connected services, and can also be used to store iOS device backups and data associated with third-party apps. iCloud-connected services allow users to create, store, access, share, and synchronize data on Apple devices or via icloud.com on any Internet-connected device. For example, iCloud Mail enables a user to access Apple-provided email accounts on multiple Apple devices and on icloud.com. iCloud Photo Library and My Photo Stream can be used to store and manage images and videos taken from Apple devices, and iCloud Photo Sharing allows the user to share those images and videos with other Apple subscribers. iCloud Drive can be used to store presentations, spreadsheets, and other documents. iCloud

Tabs enables iCloud to be used to synchronize webpages opened in the Safari web browsers on all of the user's Apple devices. iWorks Apps, a suite of productivity apps (Pages, Numbers, and Keynote), enables iCloud to be used to create, store, and share documents, spreadsheets, and presentations. iCloud Keychain enables a user to keep website username and passwords, credit card information, and Wi-Fi network information synchronized across multiple Apple devices.

43. Apple provides users with five gigabytes of free electronic space on iCloud, and users can purchase additional storage space. That storage space, located on servers controlled by Apple, may contain data associated with the use of iCloud-connected services, including: email (iCloud Mail); images and videos (iCloud Photo Library, My Photo Stream, and iCloud Photo Sharing); documents, spreadsheets, presentations, and other files (iWorks and iCloud Drive); and web browser settings and Wi-Fi network information (iCloud Tabs and iCloud Keychain). iCloud can also be used to store iOS device backups, which can contain a user's photos and videos, iMessages, Short Message Service ("SMS") and Multimedia Messaging Service ("MMS") messages, voicemail messages, call history, contacts, calendar events, reminders, notes, app data and settings, and other data. Records and data associated with third-party apps may also be stored on iCloud; for example, the iOS app for Kik, an instant messaging service, can be configured to regularly back up a user's instant messages on iCloud.

44. Based on my training and experience, my knowledge of the investigation, and the information described above, I believe that the accounts listed in this affidavit are likely to contain information relating to violations of 21 U.S.C. §§ 846 and 841(a)(1) (controlled substances) and 18 U.S.C. § 1956 (money laundering).

45. Based on the aforementioned, I believe evidentiary items can be located in the accounts described above. I request to search the account's media files, videos, text messages, call logs, address logs, address books, and any other stored information for any evidence that pertains to the possessing and distributing controlled substances and financial violations, more fully described in Attachment A, attached hereto and incorporated herein by reference.

46. The Government agrees to request another search warrant from the Court before it reviews data from the electronic storage media or electronically stored information seized pursuant to the requested warrant for purposes unrelated to this investigation.

47. Based upon my training, experience and participation in other investigations involving cocaine, crack cocaine, MDMA, steroids, methamphetamine, heroin, marijuana and/or other controlled substances, I know:

- a. That narcotics traffickers often place their assets in names other than their own to avoid detection of these assets by government agencies.
- b. That even though their assets are in other persons' names, the narcotics traffickers own and continue to use these assets and exercise dominion and control over them.
- c. That large-scale narcotics traffickers often maintain on hand large amounts of U.S. currency in order to maintain and finance their ongoing narcotics business.
- d. That narcotics traffickers often maintain books, records, notes, ledgers, airline tickets, money orders, and other papers relative to the transportation, ordering, sale, and distribution of controlled substances. That narcotics traffickers occasionally "front" (provide narcotics on consignment) narcotics to their clients. That the aforementioned books, records, receipts, notes, ledgers, etc., are often maintained where the narcotics traffickers have ready access to them, including in their residences and vehicles.
- e. That it is common for narcotics traffickers to secrete contraband, proceeds of drug sales, and records of drug transactions (some being coded and cryptic in nature and stored within electronic devices) in secure locations within, or in near proximity to, their respective residences and/or vehicles for ready access and to conceal from law enforcement authorities.
- f. That persons involved in drug trafficking often conceal in and near their residence and vehicles caches of drugs, large amounts of currency, financial instruments, precious metals, jewelry, and other items of value and/or proceeds of drug transactions; and evidence of financial transactions related to obtaining, transferring, secreting, and/or spending of large sums of money made from engaging in narcotics trafficking activities.
- g. That controlled substance traffickers commonly maintain address or telephone books or papers which reflect names, addresses and/or telephone numbers of their associates in the trafficking organization.

- h. That narcotics traffickers often utilize electronic pagers, cellular telephones, answering machines, caller identification devices, electronic address books, computers, etc., to facilitate communication with co-conspirators and/or store telephone numbers/addresses of associates, customers and sources of supply.
- i. That narcotics traffickers often possess firearms, ammunition, and other weapons.
- j. That persons present at locations where drugs are distributed, stored and/or used, often conceal many of the above mentioned items, particularly controlled substances and names/numbers of associates, on their person.

48. Based on my training and experience, I know that it is common for people involved in the sale, distribution, and use of illegal drugs to keep records of their customers and suppliers, sometimes in electronic devices.

49. I know based on my training and experience that even if long-time drug traffickers stop distributing controlled substances, either voluntarily or under law enforcement pressure, these traffickers often retain in their possession many items with evidentiary value, including telephones and telephone records; names, addresses and telephone numbers of associates; documents related to financial transactions; and other items as listed in this affidavit.

50. I know that computers and electronic storage devices may be important to a criminal investigation in two distinct ways: (1) the objects themselves may be contraband, evidence, instrumentalities, or fruits of crime, and/or (2) the objects may be used as storage devices that contain contraband, evidence, instrumentalities, or fruits of crime in the form of electronic data. In this case, I request permission to search the contents and all electronically stored information within the above-described accounts.

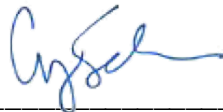
51. I believe based on the above information that individuals known and unknown are involved in drug trafficking activities and associated financial violations.

CONCLUSION

52. I respectfully request a search warrant be issued to search all contents and electronically stored information within the above-described accounts, for evidence of drug trafficking and money laundering activities in

violation of 21 U.S.C. §§ 846 and 841(a)(1) (controlled substances) and 18 U.S.C. § 1956 (money laundering), as more fully described in Attachment A hereto.

53. Based on the foregoing, I request that the Court issue the requested search warrant.



Craig Scherer, Special Agent
Homeland Security Investigations

Sworn to telephonically on the 17th day of February, 2021, at Sioux Falls, South Dakota.



VERONICA L. DUFFY
United States Magistrate Judge

UNITED STATES DISTRICT COURT
DISTRICT OF SOUTH DAKOTA
SOUTHERN DIVISION

In the Matter of the Search Regarding No. 4:21-mj-22

21-020-04

ATTACHMENTS A AND B "REDACTED"

ATTACHMENT A

This warrant applies to information associated with the Apple, Inc. account [REDACTED], that is stored at premises owned, maintained, controlled, or operated by Apple, Inc., a business with offices located at 1 Infinite Loop, Cupertino, CA 95014-2084.

ATTACHMENT B

I. Files and Accounts to be produced by Apple Inc. between January 1, 2021, to the present.

To the extent that the information described in Attachment A is within the possession, custody, or control of Apple including any messages, records, files, logs, images, videos, or information that have been deleted but are still available to Apple, Apple is required to disclose the following information to the government for each account or identifier listed in Attachment A:

a. All records or other information regarding the identification of the account, to include full name, physical address, telephone numbers, email addresses (including primary, alternate, rescue, and notification email addresses, and verification information for each email address), the date on which the account was created, the length of service, the IP address used to register the account, account status, methods of connecting, and means and source of payment (including any credit or bank account numbers);

b. All records or other information regarding the devices associated with, or used in connection with, the account (including all current and past trusted or authorized iOS devices and computers, and any devices used to access Apple services), including serial numbers, Unique Device Identifiers (“UDID”), Advertising Identifiers (“IDFA”), Global Unique Identifiers (“GUID”), Media Access Control (“MAC”) addresses, Integrated Circuit Card ID numbers (“ICCID”), Electronic Serial Numbers (“ESN”), Mobile Electronic Identity Numbers (“MEIN”), Mobile Equipment Identifiers (“MEID”), Mobile Identification Numbers (“MIN”), Subscriber Identity Modules (“SIM”), Mobile Subscriber Integrated Services Digital Network Numbers (“MSISDN”), International Mobile Subscriber Identities (“IMSI”), and International Mobile Station Equipment Identities (“IMEI”);

c. The contents of all emails associated with the account, including stored or preserved copies of emails sent to and from the account (including all draft emails and deleted emails), the source and destination addresses associated with each email, the date and time at which each email was sent, the size and length of each email, and the true and accurate header information including the actual IP addresses of the sender and the recipient of the emails, and all attachments);

d. The contents of all instant messages associated with the account, including stored or preserved copies of instant messages (including iMessages, SMS messages, and MMS messages) sent to and from the account (including all draft and deleted messages), the source and destination account or phone number associated with each instant message, the date and time at which each instant message was sent, the size and length of each instant message, the actual IP addresses of the sender and the recipient of each instant message, and

the media, if any, attached to each instant message;

e. The contents of all files and other records stored on iCloud, including all iOS device backups, all Apple and third-party app data, all files and other records related to iCloud Mail, iCloud Photo Sharing, My Photo Stream, iCloud Photo Library, iCloud Drive, iWorks (including Pages, Numbers, and Keynote), iCloud Tabs, and iCloud Keychain, and all address books, contact and buddy lists, notes, reminders, calendar entries, images, videos, voicemails, device settings, and bookmarks;

f. The activity, connection, and transactional logs for the account (with associated IP addresses including source port numbers), including FaceTime call invitation logs, mail logs, iCloud logs, iTunes Store and App Store logs (including purchases, downloads, and updates of Apple and third-party apps), messaging logs (including iMessage, SMS, and MMS messages), My Apple ID and iForgot logs, sign-on logs for all Apple services, Game Center logs, Find my iPhone logs, logs associated with iOS device activation and upgrades, and logs associated with web-based access of Apple services (including all associated identifiers);

g. All records and information regarding locations where the account was accessed, including all data stored in connection with Location Services;

h. All records pertaining to the types of service used; and

i. All records pertaining to communications between Apple and any person regarding the account, including contacts with support services and records of actions taken.

II. Information to be Seized by Law Enforcement Personnel

Any and all records that relate in any way to the email accounts described in Attachment A, which is evidence, fruits, and instrumentalities of violations of Title 21 U.S.C. §§ 841 and 846 and 18 U.S.C. § 1956, including:

a. Images, videos and other files depicting the purchase, possession, transport, shipping and/or distribution of controlled substances, to include the receipt, possession and/or transfer of proceeds.

b. Communications or documentations regarding the purchase, possession, transport, shipping and/or distribution of controlled substances, to include the receipt, possession and/or transfer of proceeds.

c. Lists of customers and contacts and related identifying information.

d. Types, amounts, and prices of drugs trafficked as well as dates, places, and amounts of specific transactions.

- e. Any information related to sources of drugs (including names, addresses, phone numbers, or any other identifying information).
- f. Any information recording schedule or travel.
- g. All financial records, Apple Cash, Apple Pay, bank records, checks, credit card bills, account information, and other financial records.
- h. Information pertaining to assets owned or under the control of the owners of the accounts being searched, including but not limited to Vehicle Identification Numbers (VINs), serial numbers and/or other identification numbers of assets.
- i. Information related to firearms and ammunition.
- j. Photographs and/or videos, in particular, photographs and/or videos of co-conspirators, assets and controlled substances.
- k. All images, messages and communications regarding wiping software, encryption or other methods to avoid detection by law enforcement;
- l. Passwords and encryption keys, and other access information that may be necessary to access the account or identifiers listed on Attachment A and other associated accounts.
- m. Evidence of user attribution showing who used or owned the device at the time the things described in this warrant were created, edited, or deleted, such as logs, phonebooks, saved usernames and passwords, documents, and browsing history.

As used above, the terms “records” and “information” include all of the foregoing items of evidence in whatever form and by whatever means they may have been created or stored, including any form of computer or electronic storage (such as flash memory or other media that can store data) and any photographic form.

III. Search Methodology

With respect to the search of the information provided pursuant to this warrant by the above-referenced provider, law enforcement personnel will make reasonable efforts to use methods and procedures that will locate and expose those categories of files, documents, communications, or other electronically-stored information that are identified with particularity in the warrant while minimizing the review of information not within the list of items to be seized as set forth herein, to the extent reasonably practicable.